(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 654 238**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **89 14560**

(51) Int Cl⁵ : G 06 K 19/073

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 07.11.89.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 10.05.91 Bulletin 91/19.

(56) **Liste des documents cités dans le rapport de recherche** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *LEFEVRE Jean Pierre* — FR.

(72) **Inventeur(s)** : LEFEVRE Jean Pierre.

(73) **Titulaire(s)** :

(74) **Mandataire** :

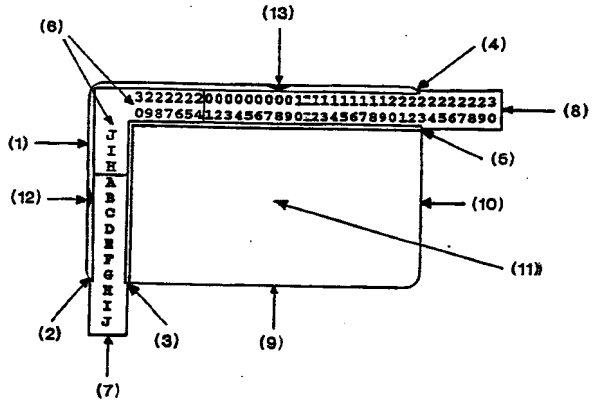
(54) Procédé d'authentification de l'identité d'une personne physique et dispositif authentificateur de mise en œuvre du procédé.

(57) L'invention concerne un procédé d'authentification et un dispositif authentificateur de mise en œuvre.

Le procédé permet de façon simple et peu coûteuse de s'assurer avec certitude de l'identité d'une personne physique, dans le cadre de l'accès aux ressources d'un système informatique protégée ou bien à celles d'un service réservé.

Le procédé permet à l'usager de faire appel à la réciprocité du mécanisme d'authentification.

En raison du mode de fonctionnement complètement autonome du dispositif authentificateur, le procédé d'authentification peut être intégré sans difficulté particulière, dans des systèmes informatiques existants ou bien dans des procédures manuelles.



FR 2 654 238 - A1

L'Invention concerne un procédé, qui permet d'authentifier avec certitude l'identité d'une personne physique, dans le cadre de l'accès aux ressources d'un système informatique protégé ou à un service réservé, et un dispositif authentificateur pour la mise en oeuvre du procédé.

Le domaine de l'invention est plus généralement celui de l'authentification réciproque d'intervenants dans le cadre de l'exécution d'une procédure d'identification mutuelle.

C'est le cas notamment, lorsqu'un usager accède à une ressource protégée d'un système informatique, par exemple la gestion de son compte bancaire depuis son domicile ou demande à bénéficier d'un service réservé à des abonnés, par exemple le service de renseignement téléphonique S.V.P.

Il est connu à ce jour, que le moyen le plus largement utilisé pour assurer le contrôle de l'identité d'une personne physique, communément dénommé "authentification", est basé sur la reconnaissance d'un code secret numérique ou alphanumérique. Ce code secret est la propriété personnelle de chaque individu.

Dans le cadre de la connexion à un système informatique, la procédure d'authentification d'un utilisateur autorisé est généralement la suivante :

- l'utilisateur communique son identité au système informatique, en composant l'identification qui lui a été attribuée, sur le clavier d'un terminal.
- dans le but de s'assurer qu'il n'y a pas usurpation d'identité, le système informatique demande à l'utilisateur de fournir une information qui lui est personnelle : son code secret.
- Le logiciel spécialisé du système informatique compare le code secret, communiqué par l'usager, avec le code secret de référence, qui est conservé dans une mémoire particulière ou dans un fichier protégé. Si les deux codes sont identiques, l'utilisateur est autorisé à accéder aux ressources du système informatique. Dans le cas contraire, l'autorisation est rejetée.

Cette procédure, bien acceptée par les usagers, présente cependant un inconvénient majeur en raison des risques de

divulgation du code secret personnel, par exemple lors de la saisie au clavier ou lors de son acheminement sur le réseau de transmission de données ou bien encore par effet de rayonnements électromagnétiques du poste de travail de l'utilisateur.

Afin de tenter de remédier à ce problème, certains prestataires de services proposent aux usagers d'introduire un second code secret. Cette disposition ne résoud pas pour autant les risques de divulgation énumérés précédemment.

Un autre inconvénient réside dans le fait, qu'en cas de divulgation du code secret personnel de l'usager il n'est pas possible de déterminer, si cette révélation provient d'une négligence due à l'usager, de l'action frauduleuse d'un tiers pour intercepter ce code secret, ou de la transmission volontaire de cette information à un tiers par l'usager lui-même. En effet du point de vue de l'implication de l'usager, le fait de disposer d'un code secret personnel n'est pas équivalent à celui de détenir un objet matériel, spécialement attribué à des fins de sécurité. Cet état de fait peu conduire à une démotivation et à un manque de participation de la part de l'usager, à l'égard des consignes de protection et de sécurité en vigueur chez le prestataire de ressources ou de services.

L'augmentation croissante des actes de piraterie ou de criminalité informatique, consécutive à l'accès illicite ou frauduleux aux systèmes informatiques, impose de renforcer le niveau de sécurité des procédures existantes, afin d'authentifier avec certitude l'identité des utilisateurs qui tentent de se connecter.

Cette obligation est encore renforcée lorsqu'il s'agit d'exécuter certaines transactions, l'accès à des programmes informatiques sensibles, à des données élémentaires confidentielles, à des ressources critiques du système d'exploitation de l'ordinateur central ou d'un ordinateur individuel.

La présente invention qui a pour objectif d'apporter une solution aux problèmes évoqués propose un procédé d'authentification et un dispositif authentificateur dont le fonctionnement est étroitement associé à ce procédé.

Ce procédé peut venir compléter la procédure décrite précédemment ou bien la remplacer en totalité.

Il est important de noter que le procédé d'authentification est particulièrement bien adapté aux opérations ayant pour objectif d'authentifier avec certitude les utilisateurs, qui accèdent aux ressources d'un système informatique, et qui souhaitent s'assurer que le système informatique accédé est bien le système informatique attendu. Cet objectif est obtenu en raison de la réciprocité du mécanisme d'authentification utilisé.

De plus, le procédé d'authentification et le dispositif authentificateur peuvent être retenus pour des objectifs de sécurité, qui justifient une authentification réciproque des intervenants, dans le cadre d'une procédure manuelle. En effet, le procédé d'authentification et le dispositif authentificateur qui le met en oeuvre, peut être avantageusement utilisé lorsque deux interlocuteurs souhaitent s'assurer avec certitude de leur identité respective, par exemple lors de la passation d'un ordre qui serait effectué par téléphone, c'est-à-dire lorsque les intervenants ne peuvent pas se reconnaître visuellement.

C'est le cas également lors de la transmission de certaines directives financières ou boursières, lorsque les interlocuteurs en présence ne sont pas toujours les mêmes, et où les conséquences d'une mystification peuvent s'avérer véritablement redoutables.

C'est également le cas dans certaines opérations de dépannage d'installations techniques effectuées à distance, par exemple la télé-maintenance d'équipements électroniques tels que des ordinateurs , des centraux téléphoniques, ou des systèmes d'informations consultables à distance.

Le procédé est notamment destiné à permettre de façon simple et peu coûteuse, d'authentifier une personne physique lorsqu'elle accède à des ressources sensibles, ou à des services réservés, en lui permettant de contrôler avec certitude, de manière réciproque, l'identité du fournisseur de la ressource protégée ou du service réservé.

D'autres caractéristiques et avantages de l'invention

ressortiront mieux de la description qui va suivre du procédé et d'un dispositif authentificateur qui le met en oeuvre, dans laquelle :

La figure 1 représente un dispositif authentificateur.

La figure 2 représente un exemple de la grille d'informations personnalisée.

La figure 3 représente une vue en coupe du dispositif authentificateur présenté dans la figure 1.

La figure 4 est un schéma qui représente les principes généraux mis en oeuvre par le procédé d'authentification et par le dispositif authentificateur.

Les figures 5, 6, et 7 représentent un exemple concret, relatif au fonctionnement du procédé d'authentification et du dispositif authentificateur.

Conformément à la figure 1, un dispositif authentificateur de mise en oeuvre du procédé est constitué d'un support rigide ayant la forme d'un rectangle de 8,5 cm de longueur sur 5,5 cm de largeur et d'environ 0,1 cm d'épaisseur.

Le dispositif authentificateur peut être réalisé dans une matière connue, plastique souple par exemple, et dans ce cas, son apparence externe est proche de celle d'une carte de crédit d'un organisme bancaire.

En ordonnée de la face supérieure (recto),il existe deux coulisses (2) et (3) dont la réalisation est faite, de manière connue, et au fond desquelles figurent des repères alphabétiques, par exemple les lettres de J à A, inscrites de haut en bas.

En abscisse de la face supérieure (recto), il existe deux coulisses (4) et (5), dont la réalisation est faite de manière connue, et au fond desquelles figurent des repères numériques, par exemple les chiffres de 30 à 01, inscrits de gauche à droite.

Dans les coulisses (2) et (3), se déplace un coulisseau (7) sur lequel figure des repères alphabétiques, par exemple les lettres de A à J inscrites de haut en bas. Le déplacement dudit coulisseau dans lesdites coulisses fait apparaître la lettre inscrite au fond des coulisses et fait disparaître de la grille, représentée par le rectangle (11), la lettre

inscrite sur la face supérieure du coulisseau. Par exemple la lettre J inscrite au fond de la coulisse apparaît lorsque la lettre J inscrite sur le coulisseau sort de la grille à la suite d'un déplacement du coulisseau (7) vers le bas. Cette action a pour effet de modifier la position de la rangée référencée A, puisque la lecture des informations s'effectue à partir de la deuxième rangée, au lieu de les obtenir à partir de la première rangée.

Dans les coulisses (4) et (5), se déplace un coulisseau (8) sur lequel figure des repères numériques, par exemple les chiffres de 01 à 30, inscrits de gauche à droite. Le déplacement dudit coulisseau dans lesdites coulisses fait apparaître les chiffres inscrits au fond des coulisses et fait disparaître de la grille représentée par le rectangle (11) les chiffres inscrits sur la face supérieure du coulisseau. Par exemple le chiffre 30, inscrit au fond de la coulisse, apparait lorsque le chiffre 30, inscrit sur le coulisseau, sort de la grille à la suite d'un déplacement du coulisseau (8) vers la droite. Cette action a pour effet de modifier la position de la colonne référencée 01, puisque la lecture des informations s'effectue à partir de la deuxième colonne de gauche, au lieu de les obtenir à partir de la première colonne de gauche.

Le rectangle intérieur (11), formé par la coulisse en ordonnée (3) et la coulisse en abscisse (5), le bord inférieur (9) et le bord droit (10) du dispositif authentificateur, est destiné à recevoir les informations imprimées qui sont spécifiques à chaque dispositif authentificateur.

L'information imprimée représentée sur la figure 2, provient du traitement informatique de personnalisation du dispositif authentificateur, qui est réalisé par la mise en oeuvre d'un algorithme spécialisé, exécuté par un ordinateur. Cette grille d'informations personnalisée est imprimée sur un support papier, qui peut être de type "non photocopiable", et dont le verso est revêtu d'un adhésif de manière a être collé sur le dispositif authentificateur, à l'emplacement référencé (11).

A la suite de cette opération, l'usager peut retrouver un

ou plusieurs caractères figurant sur la grille d'informations personnalisée, dans la mesure ou il dispose des coordonnées en abscisse et en ordonnée.

La recherche s'opère par la lecture des informations qui figurent à l'intersection des lettres A à J, inscrites sur le coulisseau positionné en ordonné, et des chiffres 01 à 30 qui sont inscrits sur le coulisseau positionné en abscisse, du dispositif authentificateur.

Le coulissement de chaque coulisseau, à des positions différentes de la position neutre, symbolisée par les flèches en ordonnée (12) et en abscisse (13), permet d'augmenter de manière considérable le nombre de combinaisons possibles qui est offert par le dispositif authentificateur.

Le positionnement de chaque coulisseau sur une lettre et sur un chiffre bien déterminé, représente un secret qui n'est connu que du seul propriétaire du dispositif authentificateur. Une fois ce positionnement assuré par l'usager, le dispositif authentificateur devient utilisable, car il permet de sélectionner correctement les caractères de la grille.

Supposons que les coordonnées de l'usager soit D 18. La mise en oeuvre du dispositif authentificateur s'opère, en positionnant la lettre D inscrite sur le coulisseau (7) en face de la flèche (12), et le nombre 18 inscrit sur le coulisseau (8) en face de la flèche (13). Il suffit ensuite de lire l'information qui figure à l'intersection formée par la coordonnée : ordonnée et abscisse.

Après usage, afin de rendre inutilisable le dispositif authentificateur par un tiers, il suffit à l'usager de replacer le dispositif authentificateur dans sa position neutre. Cette opération consiste à positionner chaque coulisseau en position de repos, c'est à dire de placer la lettre E inscrite sur le coulisseau (7) en face de la flèche (12), et le nombre 15 inscrit sur le coulisseau (8) en face de la flèche (13). De cette manière, le vol du dispositif authentificateur par une personne mal intentionnée, ne lui permettrait pas d'en faire un usage qui puisse porter atteinte au niveau de sécurité obtenu par le procédé.

Bien que chaque dispositif authentificateur soit parfai-

tement identique d'un point de vue physique, chaque dispositif authentificateur devient différent d'un point de vue logique car :

- chaque dispositif authentificateur possède une grille d'informations personnalisée inscrite dans le rectangle (11),
- chaque dispositif authentificateur ne peut être mis en oeuvre que dans la mesure ou l'usager dispose des coordonnées à positionner en ordonnée et en abscisse.

La grille d'informations personnalisée et les coordonnées spécifiques à un usager sont obtenues, à la suite d'un traitement informatique par un ordinateur, qui est effectué sur les références de l'usager, par un algorithme spécialisé.

Le dispositif authentificateur est de conception simple, ce qui est un avantage vis-à-vis de la maintenance et du coût dudit dispositif.

Le dispositif authentificateur est auditable. En effet du point de vue de la sécurité, la certitude est absolue qu'il ne peut pas y avoir de mécanisme caché, qui permettrait de dissimuler un piège quelconque, qui affaiblirait le niveau de sécurité du procédé. Il n'en est pas de même pour les dispositifs qui sont réalisés avec des composants électroniques et qui fonctionnent selon un programme enregistré. En effet rien ne prouve que ces dispositifs ne réagissent pas de manière frauduleuse dans une situation particulière. Par exemple la réception d'une séquence de caractères dont la pré-programmation, dans le dispositif électronique ou bien dans l'un des composants, a pour objectif de déclencher une action spécifique.

Le procédé d'authentification et le dispositif authentificateur pour le mettre en oeuvre, est caractérisé par le principe de base décomposé sur la figure 4, et dont l'explication est donnée ci après.

Lorsqu'un utilisateur exécute une procédure standard de connexion à un système informatique (14), le logiciel spécialisé de ce système reçoit le message composé par l'utilisateur sur le clavier de son terminal. Dans ce message est inscrit le code d'identification nécessaire, par exemple : DUCHEMIN.

Le logiciel spécialisé du système informatique mémorise ce code d'identification, et adresse en retour (15) à l'utilisateur le message représenté par la figure 5. Ce message est une suite de défis qui ont été générés de manière totalement aléatoire, et qui sont affichés sur l'écran du terminal sous la forme d'un tableau, par exemple de 10 rangées en ordonnée et de 14 colonnes en abscisse. Chaque défi est constitué lui-même de coordonnées : ordonnée et abscisse, par exemple D 23.

De manière à répondre au défi proposé par le système informatique, l'usager va exécuter les opérations suivantes :

- rechercher le défi qui lui est destiné et qui est dissimulé dans le tableau des défis (16), en utilisant les coordonnées qui lui ont été communiquées, lors de la remise de son dispositif authentificateur.
- positionner le coulisseau ordonnée (7) et le coulisseau abscisse (8) de son dispositif authentificateur en face de la lettre et des chiffres correspondants aux dites coordonnées, de manière à le mettre en concordance avec les informations dont dispose le système informatique (17).
- retrouver la séquence de caractère à fournir, en qualité de réponse, au système informatique. Ces caractères, sont situés à l'intersection de la rangée ordonnée et de la colonne abscisse, qui correspond aux coordonnées du défi (17).
- transmettre cette séquence de caractères au système informatique en la composant sur le clavier de son terminal (18).

De manière à contrôler la réponse faite par l'usager, au défi adressé par le système informatique, le logiciel spécialisé dudit système, va exécuter (19) les opérations de vérification suivantes :

- reconstituer la grille d'informations personnalisée qui est présente sur le dispositif authentificateur de l'usager, en appliquant l'algorithme spécialisé sur la référence qui identifie l'usager, par exemple DUCHEMIN.
- calculer les coordonnées de l'usager : ordonnée et abscisse en appliquant à nouveau l'algorithme spécialisé sur la référence : DUCHEMIN.
- déterminer la réponse au défi, à partir de la grille d'in-

formations personnalisée et des coordonnées : ordonnée et abscisse de l'usager.

- comparer cette réponse, avec la réponse transmise (18) par l'usager. Si les réponses sont différentes, la demande de connexion est rejetée. Si les réponses sont identiques, la demande de connexion est acceptée, puis le système va exécuter les opérations suivantes :

- déterminer la réponse du système informatique, pour répondre à la réponse formulée par l'usager; cette réponse est obtenue à partir de la grille d'informations personnalisée et des coordonnées ordonnée et abscisse de l'usager; par exemple, utiliser les informations inscrites sur la rangée située en dessous de la rangée qui correspond à la réponse au défi.

- afficher cette séquence de caractères sur l'écran du terminal de l'usager (20).

Dans le cadre d'une authentification réciproque des intervenants et de manière à vérifier la réponse proposée par le système informatique, l'usager va exécuter les opérations suivantes:

- positionner le coulisseau ordonnée (7) et le coulisseau abscisse (8) de son dispositif authentificateur en face de la lettre et des chiffres correspondants aux coordonnées qui lui ont été communiquées, lors de la remise de son dispositif authentificateur, de manière à le mettre en concordance avec les informations dont dispose le système informatique (21).

- retrouver sur la grille d'informations du dispositif authentificateur, la séquence de caractère à vérifier. Ces caractères sont situés à l'intersection de la rangée ordonnée et de la colonne abscisse.

- comparer visuellement les caractères présents sur la grille d'informations personnalisée, et les caractères qui sont affichés sur l'écran du terminal. Si les caractères sont identiques, la preuve est apportée à l'usager, que la connexion qui a été établie, est bien réalisée avec le système informatique attendu. Si les caractères affichés sont différents de ceux présents sur la grille d'informations personnalisée du dispositif authentificateur, la preuve est

apportée à l'usager, que le système informatique auquel il est connecté est un système usurpateur.

La présente invention, qui permet au système informatique de s'assurer avec certitude de l'identité de l'usager et, qui permet réciproquement à l'usager de vérifier qu'il est bien en relation avec le système informatique auquel il souhaite se connecter, sera mieux comprise à la lecture de la description qui va suivre. Cette description énumère les actions à exécuter dans le cadre d'un exemple concret, non limitatif du procédé et du dispositif authentificateur qui le met en oeuvre, et fait référence aux informations qui sont représentées sur la figure 5, la figure 6 et la figure 7.

Nous supposerons dans cet exemple que :

- les coordonnées de l'usager DUCHEMIN sont B 08, c'est-à-dire que l'algorithme spécialisé a déterminé, à partir de la chaîne de caractères DUCHEMIN, la lettre B en ordonnée et les chiffres 08 en abscisse.
- la convention existante, entre le système informatique et l'usager, pour répondre au défi, consiste à échanger les quatre lettres de droite qui figurent à l'intersection : ordonnée et abscisse, de la grille d'informations personnalisée.
- la convention existante, entre le système informatique et l'usager, pour répondre à la réponse au défi, consiste à échanger les quatre lettres de droite de la ligne inférieure à celle de l'intersection : ordonnée et abscisse de la grille d'informations personnalisée.

Afin de découvrir le défi qui est dissimulé dans l'écran affiché sur son terminal, l'usager recherche, dans la rangée B et dans la colonne 08 du tableau proposé, les coordonnées correspondantes à ce défi. La consultation du tableau de la figure 5 lui indique par conséquent les coordonnées : F 13.

Afin de rechercher la réponse à ce défi, l'utilisateur doit au préalable rendre utilisable son dispositif authentificateur, en le positionnant avec les coordonnées qui lui ont été communiquées, dans notre exemple B 08.

La figure 6 représente le dispositif authentificateur au repos. Les coordonnées F 13 donnent accès aux quatre carac-

tères EBUZ. Cette réponse ne correspond pas au défi F 13 qui a été proposé par le système informatique.

La figure 7 représente le dispositif authentificateur en position de fonctionnement. Le coulisseau placé en ordonnée est positionné sur la lettre B, et le coulisseau placé en abscisse est positionné sur les chiffres 08. Les coordonnées F 13 donnent à présent accès aux quatre caractères HBXP. Cette réponse correspond au défi F 13 qui a été proposé par le système informatique.

Afin d'apporter la preuve à l'usager que la connexion qui est établie, est bien réalisée avec le système informatique attendu, le système retourne à l'usager, la réponse de la réponse HBXP au défi F 13, dans notre exemple les quatres caractères situés sur la rangée suivante - la rangée G - et ayant pour origine la même ordonnée. Le système communique par conséquent les lettres UYTM, en les affichant sur l'écran du terminal de l'utilisateur.

A ce stade, l'usager peut comparer visuellement, la réponse transmise par le système informatique, et celle que lui procure son disposif authentificateur. En fonction du résultat de cette vérification, l'usager décide ou non de poursuivre son activité.

Enfin, dans le but de rendre inutilisable le dispositif authentificateur, par un tiers non autorisé, l'usager replace chaque coulisseau dans la position neutre, qui est décrite sur la figure 6.

Un autre exemple, de convention entre le système informatique et l'usager, peut consister à échanger des informations dynamiques, c'est-à-dire des informations qui changent en permanence. Dans ce cas la grille d'informations spécialisée est constitué de séquence de chiffres. Le défi adressé à l'usager consiste à ce qu'il additionne deux séries de chiffres et qu'il retourne le résultat, en qualité de réponse, au défi proposé par le système informatique. Le défi est communiqué à l'usager de la manière habituelle, sous la forme d'un tableau de défis. Le premier terme à additionner est obtenu par la lecture des chiffres à l'intersection des coordonnés : ordonnée et abscisse de la

grille d'informations personnalisée, avant que le coulisseau ordonnée et le coulisseau abscisse ne soit positionné. Le second terme à additionner est obtenu, quand à lui, par la lecture des chiffres à l'intersection des coordonnés : ordonnée et abscisse de la grille d'informations personnalisée, après que le coulisseau ordonnée et le coulisseau abscisse sont positionnés. La réponse est représentée par le résultat de l'opération. A partir de cette réponse, il est pratiquement impossible de retrouver les termes d'origines. La réponse du système informatique à l'usager est le résultat de la multiplication des deux termes précédemment additionnés par l'usager. Ainsi, l'usager peut aisément authentifier le système informatique qui vient de formuler la réponse.

Le procédé d'authentification utilise un dispositif authentificateur tel que représenté par la figure 1. Dans ce cas le support est une matière plastique souple. Cependant, une caractéristique complémentaire et avantageuse du procédé consiste en ce que le dispositif authentificateur puisse être réalisé avec des médias différents. Par exemple, la logique retenue pour le dispositif authentificateur peut être trancrite dans un logiciel. Dans le but à terme, d'être exécuté par un ordinateur généralisé, ou par un ordinateur spécialisé, ce logiciel peut lui même être enregistré dans l'un des médias suivants :

- un composant électronique spécialisé tel qu'une mémoire de type RAM ou EPROM ou bien encore EEPROM
- un support de type magnétique, par exemple une disquette d'ordinateur personnel au format standard de 5 pouces 1/4, de 3 pouces 1/2 ou de 2 pouces 1/2.
- un support de type optique pour ordinateur personnel,
- un support de type photographique, par exemple une carte à laser,
- un micro-calculateur,
- etc ...

Cependant du point de vue de l'usager, le mode opératoire, qui préside à la mise en oeuvre du média, reste identique à celui du dispositif authentificateur, lequel est

transposé dans son intégralité.

Il est évident par ailleurs, que tout procédé d'authentification d'une personne physique, mis en oeuvre ou non par un dispositif authentificateur, serait réputé être réalisé dans le même esprit que celui de l'invention, et par conséquent ne sortirait pas du cadre de ladite invention, si l'une ou plusieurs des spécifications techniques étaient modifiées par :

- la densité des informations inscrites sur la grille d'informations personnalisée,
- la présentation des informations inscrites sur la grille d'informations personnalisée,
- la nature des informations inscrites sur la grille d'informations personnalisée,
- la densité des informations affichées sur l'écran du terminal,
- la présentation des informations affichées sur l'écran du terminal,
- la nature des informations affichées sur l'écran du terminal,
- les caractéristiques particulières à un ou plusieurs des algorithmes utilisés,
- le nombre de lettres inscrit sur le coulisseau placé en ordonnée,
- le nombre de chiffres inscrit sur le coulisseau placé en abscisse,
- la séquence de présentation des lettres qui figurent sur le coulisseau placé en ordonnée,
- la séquence de présentation des chiffres qui figurent sur le coulisseau placé en abscisse,
- les conventions qui concernent l'emplacement et la longueur du défi affiché sur l'écran du terminal de l'utilisateur,
- les conventions qui concernent l'emplacement et la longueur du défi présent sur la grille d'informations personnalisée,
- les conventions qui concernent l'emplacement et la longueur de la réponse au défi présent sur la grille d'informations personnalisée,
- les conventions qui concernent l'emplacement et la longueur

de la réponse, faite par le système informatique, à la réponse au défi,

- la suppression du coulisseau en ordonnée, au bénéfice d'une représentation fixe des lettres A à J ou de tout autres lettres,

- la suppression du coulisseau en abscisse, au bénéfice d'une représentation fixe des chiffres 01 à 30 ou de tout autres chiffres,

- le nombre de rangées qui sont disposées en ordonnée de la grille d'informations personnalisée et du coulisseau ordonnée qui lui correspond,

- le nombre de rangées qui sont disposées en abscisse de la grille d'informations personnalisée et du coulisseau abscisse qui lui correspond.

L'invention propose un procédé d'authentification et un dispositif authentificateur de mise en oeuvre, acceptable par tous et qui, en raison de la parfaite autonomie du dispositif authentificateur, ne présente pas de difficulté particulière pour l'intégrer dans des installations, des procédures, des équipements en service à ce jour ou pour l'implanter dans de nouveaux produits.

Le procédé d'authentification et le dispositif authentificateur qui le met en oeuvre est destiné à permettre de façon simple et peu coûteuse de s'assurer avec certitude de l'identité d'une personne physique, et lui permet de plus, de faire appel à la réciprocité du mécanisme d'authentification. Le procédé concerne les moyens d'authentification à niveau de sécurité élevé.

REVENDICATIONS

1) Procédé d'authentification caractérisé en ce qu'il consiste en la réalisation des étapes suivantes :

a) faire produire par un système informatique, une suite de défis puis les afficher sur un écran spécialisé.

b) faire rechercher par un usager, le défi qui lui est destiné et qui est dissimulé dans un tableau de défis.

c) faire rechercher par un usager, à l'aide de son dispositif authentificateur, la réponse au défi qui lui est proposé.

d) faire vérifier par le système informatique, la réponse de l'usager.

e) faire répondre par le système informatique, à la réponse formulée par l'usager, si cette réponse est conforme.

f) faire vérifier par l'usager, à l'aide de son dispositif authentificateur, la réponse formulée par le système informatique.

2) Procédé selon la revendication 1 caractérisé en ce que l'étape a) relative à la création des défis par le système informatique, génére de manière totalement aléatoire la suite des défis, et les affiche sur l'écran spécialisé d'un terminal ou d'un poste de travail, sous la forme d'un tableau de défis qui est constitué de rangées en ordonnée et de colonnes en abscisse.

3) Procédé selon la revendication 1 caractérisé en ce que l'étape b) relative à la recherche par un usager, pour découvrir le défi qui lui est destiné et qui est dissimulé dans le tableau des défis, s'effectue en utilisant les coordonnées secrètes : ordonnée et abscisse, qui lui ont été communiquées confidentiellement.

4) Procédé selon la revendication 1 caractérisé en ce que l'étape c) relative à la recherche par un usager, pour découvrir la réponse au défi qui lui est proposé par le système informatique, s'opère par la mise en oeuvre du dispositif authentificateur, qui a été spécialement attribué à l'usager.

La réponse à ce défi se trouve dans la grille d'informations personnalisée, qui figure sur le dispositif authentificateur,

à l'intersection de la rangée ordonnée et de la colonne abscisse, laquelle intersection correspond aux coordonnées du défi,

5) Procédé selon la revendication 1 caractérisé en ce que l'étape d) relative à la vérification de la réponse de l'usager par le système informatique, consiste en la réalisation des étapes suivantes :

- reconstituer la grille d'informations personnalisée, qui figure sur le dispositif authentificateur de l'usager, en appliquant l'algorithme spécialisé sur la référence qui identifie l'usager.
- calculer les coordonnées de l'usager : ordonnée et abscisse en appliquant à nouveau l'algorithme spécialisé sur la référence qui identifie l'usager.
- déterminer la réponse exacte au défi, à partir de la grille d'informations personnalisée et des coordonnées de l'usager : ordonnée et abscisse.
- comparer cette réponse, avec la réponse transmise par l'usager. Si les réponses sont différentes, la demande de connexion est rejetée. Si les réponses sont identiques, la demande de connexion est acceptée.

6) Procédé selon la revendication 1 caractérisé en ce que l'étape e) relative à la réponse que fait le système informatique, pour répondre à la réponse formulée par l'usager, consiste en la réalisation des étapes suivantes :

- reconstituer la grille d'informations personnalisée, qui figure sur le dispositif authentificateur de l'usager, en appliquant l'algorithme spécialisé sur la référence qui identifie l'usager.
- calculer les coordonnées de l'usager : ordonnée et abscisse en appliquant à nouveau l'algorithme spécialisé sur la référence qui identifie l'usager.
- déterminer la réponse à fournir, à partir de la grille d'informations personnalisée et des coordonnées de l'usager : ordonnée et abscisse, en utilisant les informations inscrites sur la rangée située au dessous de la rangée qui correspond à la réponse au défi.
- afficher cette séquence de caractères sur l'écran spécia-

lisé du terminal ou du poste de travail de l'usager.

7) Procédé selon la revendication 1 caractérisé en ce que l'étape f) relative à la vérification par l'utilisateur, de la réponse formulée par le système informatique, s'opère par la mise en oeuvre du dispositif authentificateur, qui a été spécialement attribué à l'usager.

Cette réponse se trouve dans la grille d'informations personnalisée, qui figure sur le dispositif authentificateur, sur la rangée située au dessous de la rangée qui correspond aux coordonnées du défi, lequel défi est à l'intersection de la rangée ordonnée et de la colonne abscisse.

8) Dispositif authentificateur pour mise en oeuvre du procédé selon l'ensemble des revendications précédentes, caractérisé en ce qu'il comporte, sur un support en forme de rectangle de 8,5 cm de longueur, de 5,5 cm de largeur et d'une épaisseur d'environ 0,1 cm, fabriqué dans une matière connue, les éléments suivants :

- deux coulisses, dont la réalisation est faite de manière connue, qui sont placées sur la face supérieure (recto) en ordonnée gauche (2) et en ordonnée droite (3), et au fond desquelles figurent des repères alphabétiques, par exemple les lettres de J à A inscrites de haut en bas.
- un coulisseau (7) sur lequel figure des repères alphabétiques, par exemple les lettres de A à J, inscrites de haut en bas, qui se déplace dans les coulisses placées en ordonnée (2) et (3).

Le déplacement dudit coulisseau dans lesdites coulisses fait apparaître la lettre inscrite au fond des coulisses, et fait disparaître la lettre inscrite sur la face supérieure du coulisseau.

- deux coulisses, dont la réalisation est faite de manière connue, qui sont placées sur la face supérieure (recto) en abscisse supérieure (4) et en abscisse inférieure (5), et au fond desquelles figurent des repères numériques, par exemple les chiffres de 30 à 01, inscrits de gauche à droite.
- un coulisseau (8) sur lequel figure des repères numériques, par exemple les chiffres de 01 à 30, inscrits de gauche à droite, qui se déplace dans les coulisses placées en abscisse

(4) et (5).

Le déplacement dudit coulisseau dans lesdites coulisses fait apparaître les chiffres inscrits au fond des coulisses, et fait disparaître les chiffres inscrits sur la face supérieure du coulisseau.

- un logement en forme de rectangle (11), formé par les coulisses en ordonnée (3), en abscisse (5), le bord inférieur (9), et le bord droit (10), du dispositif authentificateur, qui est destiné à recevoir la grille d'informations personnalisée laquelle est spécifique pour chaque dispositif authentificateur.

9) Dispositif authentificateur selon la revendication 8 caractérisé en ce que :

- le déplacement du coulisseau (7) dans les coulisses (2) et (3) a pour effet de modifier la position de la rangée référencée A, puisque la lecture des caractères sur la grille d'informations personnalisée s'effectue à partir de la deuxième rangée au lieu de les obtenir à partir de la première rangée.

- le déplacement du coulisseau (8) dans les coulisses (4) et (5) a pour effet de modifier la position de la colonne référencée 01, puisque la lecture des caractères sur la grille d'informations personnalisée s'effectue à partir de la deuxième colonne de gauche au lieu de les obtenir à partir de la première colonne de gauche.

- le coulissemement de chaque coulisseau à des positions différentes de la position neutre, symbolisée par les flèches en ordonnée (12) et en abscisse (13) permet d'augmenter de manière considérable le nombre de combinaisons possibles qui est offert par le dispositif authentificateur.

- le positionnement de chaque coulisseau sur une lettre et sur un chiffre bien déterminé, représente un secret, qui n'est connu que du seul propriétaire du dispositif authentificateur. Une fois ce positionnement assuré par l'usager, le dispositif authentificateur devient utilisable, car il permet de sélectionner correctement les caractères de la grille d'informations spécialisée. A l'inverse, afin de rendre inutilisable le dispositif authentificateur par un

tiers, il suffit à l'usager de replacer le dispositif authentificateur dans sa position neutre. Cette opération consiste à positionner chaque coulisseau en position de repos, c'est à dire de placer la lettre E inscrite sur le coullisseau (7) en face de la flèche (12), et le nombre 15 inscrit sur le coulisseau (8) en face de la flèche (13).

10) Dispositif authentificateur selon la revendication 8 caractérisé en ce que :

- chaque dispositif authentificateur possède une grille d'informations personnalisée inscrite dans le rectangle (11). Cette grille résulte du traitement informatique de personnalisation, qui est réalisé par la mise en oeuvre d'un algorithme spécialisé, exécuté par un ordinateur, et appliqué sur la référence qui identifie l'usager. Cette grille d'informations est imprimée sur un support papier, dont le verso est revêtu d'un adhésif de manière a être collé dans le rectangle (11).
- chaque dispositif authentificateur ne peut être mis en oeuvre que dans la mesure ou l'usager connait les coordonnées à positionner en ordonnée et en abscisse.

Lesdites coordonnées spécifiques à un usager sont obtenues, à la suite d'un traitement informatique par un algorithme spécialisé, exécuté par un ordinateur, et appliqué sur la référence qui identifie l'usager. Lesdites coordonnées sont communiquée de manière confidentielle audit usager.

PLANCHE 1/3

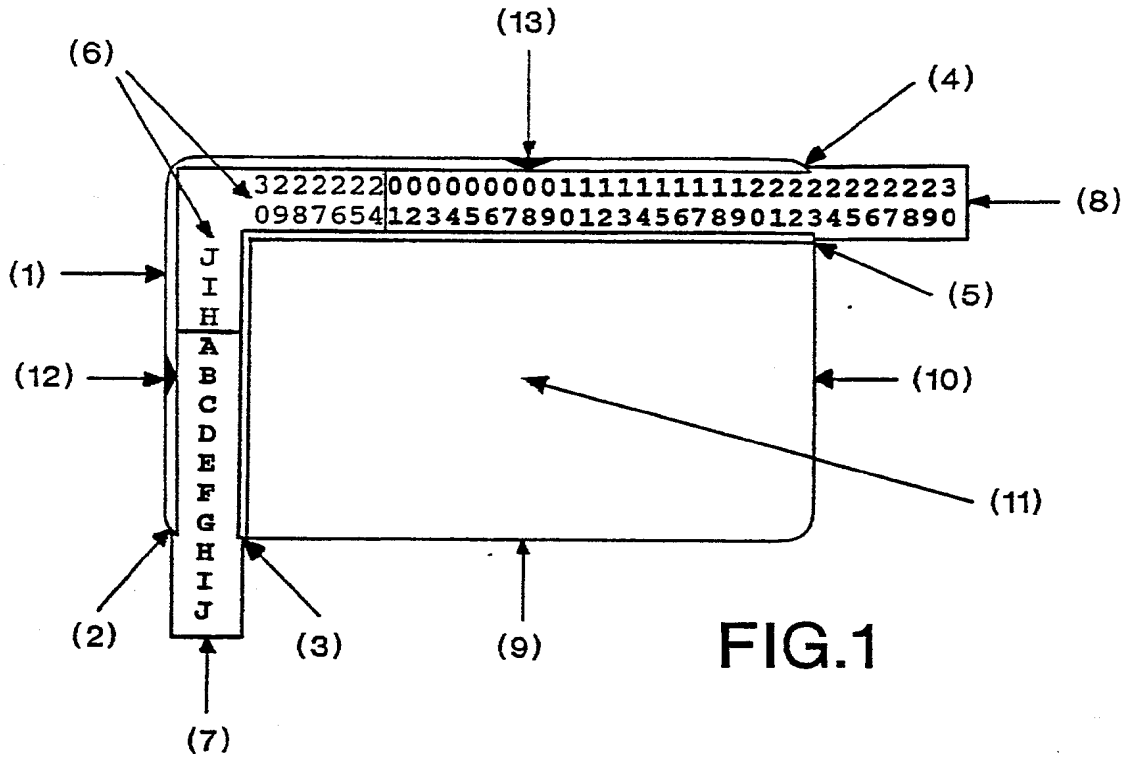


FIG.1

SNSCRFAIPBVJMINHDMJSQKRWXNFZSG
FLGQDQAFJBWAXYWKAZXLEILTTLFMKZ
GQQYYTVKDRAUPQIDPPBHPSHCBTGQMP
DEASYHEVCEQZVHXSEFNLTDTJULKWAE
ZBVWXBJVLJGSWGJWPSRANTFGBIIEPN
RFQASKYGFBYBEBUZCMPFMQEFKYIDEE
EBMPAIFHQSEPDQPDAPVWWJQIGFPRZL
JWHVPWPZGWSQAEQGIYWRHPRJPPMUWO
BFIXNUBYPRKXZHUISZUHBXPKTYMCNP
GBIPRDWAKNMGHRSXPKHUYTMLQWXUJE

FIG.2

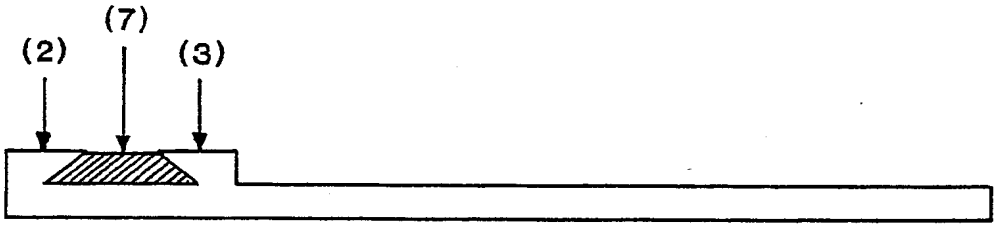
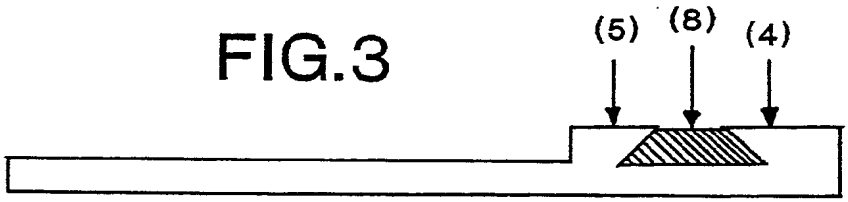


FIG.3



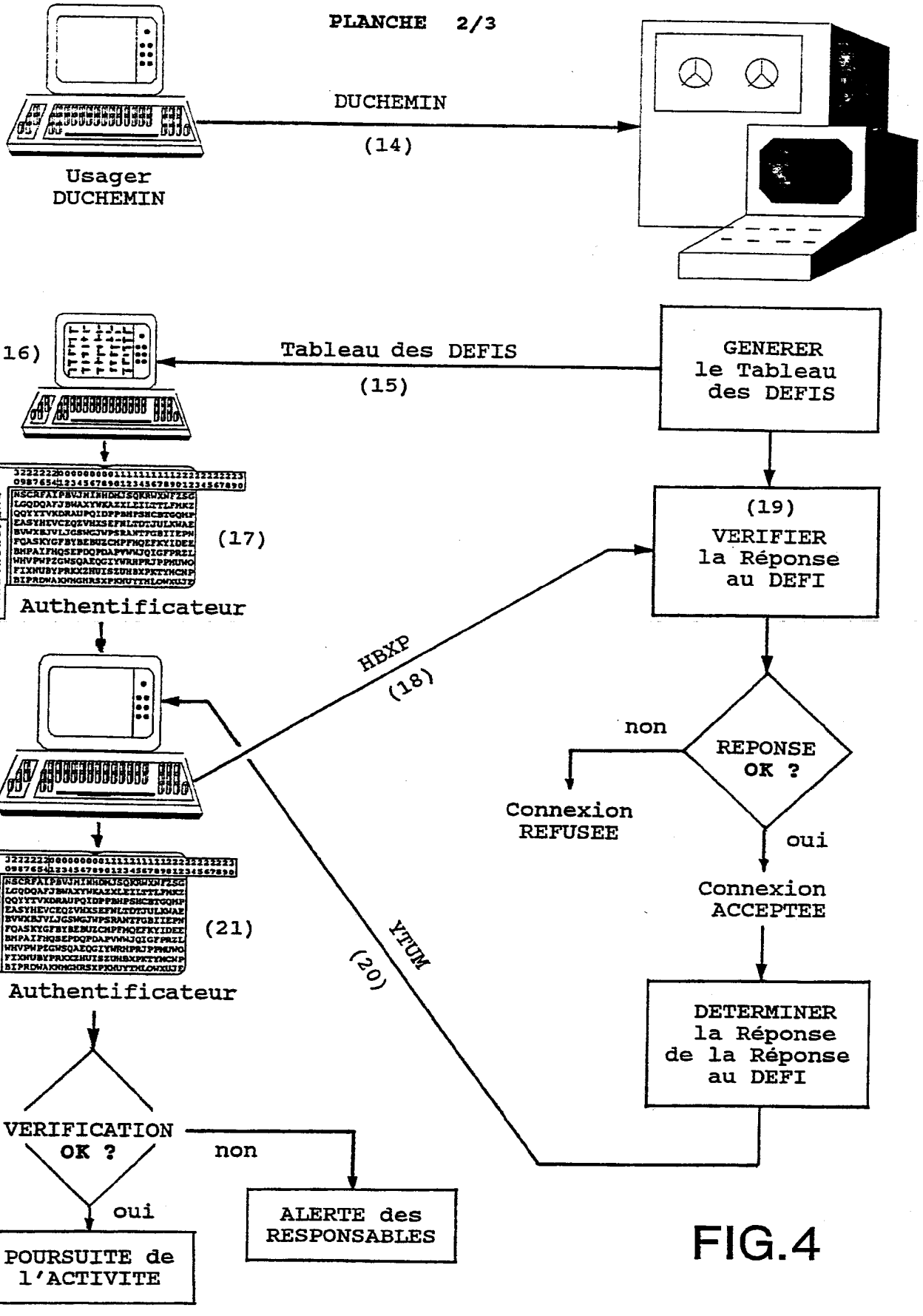


FIG.4

PLANCHE 3/3

FIG.5

	01	02	03	04	05	06	07	08	09	10	11	12	13	14
A	D19	E14	D26	F05	J17	B15	H09	G23	A11	C20	I13	F04	C15	E29
B	C22	G03	F14	I09	H26	B19	A04	F13	C08	A22	F01	G17	B25	C12
C	B07	H15	G21	D07	A12	C22	F15	G17	A29	I17	B18	C18	F21	D13
D	C25	D16	H13	I18	C06	B24	C01	A08	I19	B12	C06	G29	A07	F23
E	D14	H13	C12	D15	E19	H25	E13	B11	C23	E07	H28	I17	A10	J26
F	F03	G07	H09	F09	B23	C16	F11	C18	F27	H19	G18	J15	C17	D16
G	D05	F14	J05	E07	C04	I09	J22	C15	F25	G12	D14	I17	E16	J17
H	E10	B03	C12	I24	G19	J01	D15	B04	A24	F13	G22	D06	G07	B12
I	F20	D09	J13	G28	F12	H13	J26	F20	D17	C18	D12	A06	C27	H15
J	E13	D25	C18	J24	A02	B29	I24	J15	D22	E18	F06	C13	D11	J25

FIG.6

```
                    ▼
     0000000001111111111222222222223
     1234567890123456789012345678 90
  A  SNSCRFAIPBVJMINHDMJSQKRWXNFZSG
  B  FLGQDQAFJBWAXYWKAZXLEILTTLFMKZ
  C  GQQYYTVKDRAUPQIDPPBHPSHCBTGQMP
  D  DEASYHEVCEQZVHXSEFNLTDTJULKWAE
► E  ZBVWXBJVLJGSWGJWPSRANTFGBIIEPN
  F  RFQASKYGFBYBEBUZCMPFMQEFKYIDEE
  G  EBMPAIFHQSEPDQPDAPVWWJQIGFPRZL
  H  JWHVPWPZGWSQAEQGIYWRHPRJPPMUWO
  I  BFIXNUBYPRKXZHUISZUHBXPKTYMCNP
  J  GBIPRDWAKNMGHRSXPKHUYTMLQWXUJE
```

FIG.7

```
                    ▼
     3222222000000000111111111222222222223
     0987654123456789012345678901234567890
  J  SNSCRFAIPBVJMINHDMJSQKRWXNFZSG
  I  FLGQDQAFJBWAXYWKAZXLEILTTLFMKZ
  H  GQQYYTVKDRAUPQIDPPBHPSHCBTGQMP
  A  DEASYHEVCEQZVHXSEFNLTDTJULKWAE
► B  ZBVWXBJVLJGSWGJWPSRANTFGBIIEPN
  C  RFQASKYGFBYBEBUZCMPFMQEFKYIDEE
  D  EBMPAIFHQSEPDQPDAPVWWJQIGFPRZL
  E  JWHVPWPZGWSQAEQGIYWRHPRJPPMUWO
  F  BFIXNUBYPRKXZHUISZUHBXPKTYMCNP
  G  GBIPRDWAKNMGHRSXPKHUYTMLQWXUJE
  H
  I
  J
```

REPUBLIQUE FRANÇAISE

2654238

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FR 8914560
FA 434101

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
A	GB-A-2198567 (GARDINER,CHRISTIE) * page 6, ligne 30 - page 8, ligne 5; figure 1 *	1, 4-6, 8-10
A	FR-A-2582421 (LEFEVRE) * page 5, ligne 10 - page 6, ligne 36; figure 2 *	1, 4-6
A	FR-A-2617303 (JOSSE) * page 1, lignes 1 - 32; figures 1-3 *	1

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G06F
G07F
G07C

Date d'achèvement de la recherche	Examinateur
16 JUILLET 1990	HERBELET J.C.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1

EPO FORM 1503 03.82 (P0413)